UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of:
6412 103rd Avenue, Kenosha, Wisconsin

Case No. 16M064

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property:

See Attachment A

located in the Eastern District of Wisconsin, there is now concealed:

See Attachment B

The basis for the search under Fed. R. Crim P. 41(c) is:

- ■ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to violations of: Title 18 United States Code, Sections 2252(a)(1), (a)(2) and (a)(4)(B)
Receipt, Distribution and Possession of Child Pornography

The application is based on these facts: See attached affidavit.

Aaron Koehler
Applicant's signature

Special Agent Aaron Koehler, ICAC
Printed Name and Title

Sworn to before me and signed in my presence:

Date: April 29, 2016

Judge's signature

City and State: Milwaukee, Wisconsin

David E. Jones, U.S. Magistrate Judge
Printed Name and Title

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Aaron Koehler, being duly sworn on oath, depose and state as follows:

BACKGROUND

1. I am a Special Agent (SA) with the State of Wisconsin, Department of Justice, Internet Crimes Against Children (ICAC), Division of Criminal Investigation and have been employed as a SA since October of 2012. Prior to my appointment as a SA, I was employed as a Police Officer with the City of Beloit Police Department between July of 2008 and October of 2012. Throughout my law enforcement career, I have gained experience working complex criminal investigations, including internet crimes committed against children, sexual assault of children and adults, financial crimes, death investigations, and narcotics trafficking and most recently was assigned to the Wisconsin Internet Crimes Against Children Task Force (ICAC), which was developed pursuant to a federal grant received from the Office of Juvenile Justice and Delinquency Prevention and NCMEC. ICAC's primary responsibility is the investigation of sexual crimes committed against children through the use of a computer and the Internet. I have participated in numerous search warrants related to child exploitation, including the possession of child pornography.

2. In October of 2012, I received 24 hours of training on the sexual exploitation and abuse of children from experienced ICAC Special Agents with Division of Criminal Investigation. This training included basic computer skills; introduction to ICAC investigations; child sex trafficking; peer to peer child pornography investigations; basic forensic computer examination; digital evidence collection; undercover chat investigations, interviewing children and suspects in ICAC investigations; social networking trends; and CyberTipline investigations. In April of 2014, I received 8 hours of training regarding operational skills and investigative tactics in child exploitation cases. In August of 2014 and 2015, I received approximately 64 hours of training at the

Crimes Against Children conference in Dallas, Texas, and attended multiple classes related to the investigation of Internet Crimes against Children. In October of 2014, I attended 40 hours of training regarding the investigation of Internet Crimes Against Children, based on curriculum assembled by the Wisconsin Department of Justice-Division of Criminal Investigation. In January of 2015, I attended the Wisconsin Department of Justice, Division of Criminal Investigation undercover chat class and received approximately 20 hours of training in conducting online undercover investigations. In September of 2015, I attended approximately 24 hours of training hosted by the United States Department of Justice in Green Bay, Wisconsin, regarding interview techniques when related to child exploitation. Also in September of 2015, I met with representatives from various ESPs and analysts from NECMEC in an effort to further understand and improve CyberTipline reports. Furthermore, I have received 160 hours of training from the Wisconsin Department of Justice, Division of Criminal Investigation in the basic investigation of crimes. I have also provided training to local and federal law enforcement in regard to the investigation of ICAC.

3. I seek a search warrant for the premises 6412 103rd Avenue, Kenosha, Wisconsin (hereinafter Target Location and described in Attachment A) to search for and seize the items and evidence set forth in Attachment B. Based upon the information summarized in this affidavit, I have reason to believe that evidence of certain crime(s), to wit: Receipt, Distribution and Possession of Child Pornography, committed in violation of Title 18, United States Code, Sections 2252 (a)(1), (a)(2) and (a)(4)(B).

4. The facts in this affidavit come from my personal observations, information provided to me by the Electronic Service Provider (ESP), Facebook Inc., via the National Center for Missing and Exploited Children (NCMEC) CyberTipline Report submitted by Facebook Inc., records

subpoenaed from Time Warner Cable LLC, records obtained, and reports compiled by the United States Department of Homeland Security-Investigations (HSI), that were provided to me in an official capacity, and corporate and government entities. I believe the information I obtained from other sources is truthful and reliable, in that such information was collected and provided by persons or entities in the performance of their official duties, or in the course of normal business operations. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

BACKGROUND INFORMATION ON THE DIGITAL EXPLOITATION OF CHILDREN

5. Based on my training, experience and discussions with senior ICAC law enforcement officers, I know the following:

A. The primary manner in which child pornography is produced, distributed, and possessed is through the use of computers and the Internet. Child pornographers produce both still and moving images directly from common video, cell/smart phone and/or digital cameras. These digital recording devices can be connected to a computer, and through the use of various software programs, images and videos can be transferred directly to a computer, transferred to another computer via the Internet, and/or can be stored directly onto a computer or other electronic storage devices. Individuals with an interest in child pornography can obtain videos and images through other entities that make their videos and images of child pornography available for purchase through the Internet and will mail said materials to individuals willing to pay for them.

B. Individuals that possess, receive, transfer and distribute child pornography and participate in chat rooms, social networking, and instant messaging use communication devices known as a modem or cable connections that allow any computer to connect to another computer

by telephone line, cable, or wireless service. By connection to an Internet service provider (ISP), electronic contact can be made to millions of computers around the world. Internet service providers are sometimes commercial concerns, which allow subscribers to dial local numbers and connect to a network, which is connected to their host systems. These ISP's allow electronic mail/messaging service between subscribers, and usually between their own subscribers and those of other networks. Once one has subscribed to an Internet service provider, it costs nothing to send or receive image, video or text files.

C. Each image, video or text file is a digital duplicate of the computer original; therefore, a perpetrator's child pornography is not diminished if he or she distributes the pornography to others via computer. Internet access also allows the computer user to locate and communicate with others of similar inclination. Once contact is established, it is then possible to send text messages and graphic images and videos to others. These communications can be quick, relatively secure and as anonymous as desired.

D. The ability to store images and videos in a digital form makes the computer an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown exponentially within the last several years. Hard drives with a capacity of one thousand (1000) gigabytes (also known as a terabyte) are not uncommon, and these drives can store thousands of images at a very high resolution.

E. Images and videos can be electronically sent to anyone with access to a computer and Internet connection, and can be downloaded onto computers for ease of storage, duplication, and distribution. With the proliferation of commercial enterprises providing Internet service, computer transfer and digital copying is the preferred method of distributing child pornography. The capacity of computer hard drives, the ease of access and relative anonymity afforded the

computer user permits individuals with an interest in child pornography to amass large amounts of such materials. Those materials can be saved indefinitely on various electronic storage devices, transferred from one storage device to another, and/or transferred electronically to remote storage locations commonly referred to as the "cloud." I also know that computers and other storage devices can be very small in size and therefore can be easily transported and easily stored in just about any location, including a vehicle. Furthermore, offenders can often keep these devices with them at virtually all times, including when driving a vehicle.

F. Each time an individual views an online digital image or video or participates in chat rooms, social networking, or instant messaging, that image or video and chat log or instant message, or remnants of that image or video and chat log or instant message, is stored in the hard drive of the computer used to view the image or video and participate in a chat or instant message. A forensic examination of such a hard drive can identify and retrieve such images or videos and chat or instant message logs, including those images or videos of child pornography, even if those images or videos have been deleted by the computer operator.

G. Individuals involved in child pornography will use places that they consider private and secure to produce, receive, download, store, and/or view pornographic images or videos, and/or participate in chat rooms, social networks, or instant messaging available on the Internet. The majority of cases the private and secure place is the individual's residence.

H. Individuals who have a sexual interest in children often seek out, possess and/or collect child pornography, in that those images or videos provide them with sexual stimulation, gratification, and satisfaction. In addition, individuals who have a sexual interest in children may also seek out children on the Internet via social sites or chat rooms, befriend those children, expose those children to sexual content (including but not limited to sexually explicit electronic

messaging and sexually explicit web camera sessions) and attempt to meet with those children in person in order to satisfy their sexual appetite for children. These same individuals may also use digital technology to seek out others who share the same sexual desires in order to trade and/or distribute images of child pornography, and/or provide access or introductions to actual children for sexual assault or other forms of exploitation.

I. Individuals who are involved with child pornography are not likely to voluntarily dispose of all of the images they possess, as those images are viewed as prized and valuable materials, regardless of the amount of time that has passed since they acquired the materials. Offenders may also winnow their materials to keep and save the images and/or videos that are the most satisfying or sexually arousing to them. Those individuals are likely to seek out additional images to satisfy their sexual appetites; as mentioned earlier, their ability today to seek out and obtain additional child pornography is unprecedented because of the Internet. I know from training and experience that such individuals have been known to maintain possession of their child pornography for years, even decades. Individuals who have an appetite for child pornography are likely to always have that desire, and that given the circumstances and opportunity, such individuals often molest children as well.

J. A suspect's lack of a prior history of child-related sex offenses is not a determining factor in the outcome of these investigations.

K. Computer/digital technology continues to advance, and it is common for users to upgrade their computers or digital devices or purchase new ones. This reality does not mean that the passage of time or changes in technology make it less likely that an offender retains evidence of child sexual exploitation because, as explained earlier, individuals with a sexual interest in children and child pornography will likely always have that interest and therefore seek out and

save contraband materials in order to satisfy their ongoing desires. I also know from personal and professional experience and training that when a new computer or other digital device is purchased, the purchaser can easily save valued data located on the device being replaced by either saving the device itself or the storage media from the device (e.g., the hard drive of a computer) or by copying that data from the old device to the new device or to other digital storage media. Once a person owns and uses digital devices, including computers and/or cell phones, they do not get rid of those products as they become an essential part of their personal and/or professional lives. While persons will change their Internet and/or cell phone service providers, they do not do so to abandon technology, but rather to subscribe to another provider that could provide better service and/or prices for those services.

L. The professionally accepted method for conducting a complete forensic examination of computers, computer media and other electronic devices is to first make a forensically sound copy of the contents of the storage media associated with the device, if possible, and that the creation of that copy can take hours, depending on the amount of data stored there, and requires specialized equipment. Furthermore, the actual forensic examination of the contents of any seized device is likely to be a time intensive task ordinarily conducted in DCI investigations by DCI computer forensic analysts with training and expertise in digital forensics at the secure DCI computer forensic laboratory, where the analysts have access to powerful computers and other materials designed to assist in the analysis and protect the integrity of the evidence. These analysts are very often not sworn law enforcement officers. A requirement that the analysts conduct the entirety of their analysis process at the scene of the search authorized by the requested search warrant would create a significant and unjustified burden on law enforcement resources and on the property owner and would be contrary to the usual principle that law

enforcement searches be as brief and non-intrusive as possible. For these reasons, I specifically request that the court expressly authorize law enforcement to seize all items, consistent with the things to be searched for and seized as described in Attachment B, the contents of any digital device or media later and analyze the same in a manner consistent with generally accepted practices in the field of computer forensics.

FACTS ESTABLISHING PROBABLE CAUSE

6. On September 18, 2015, I met with United States Department of Homeland Security Investigations (HSI)-Milwaukee SA Steve Westover regarding an HSI investigation he wished to pass to DCI-Milwaukee. SA Westover provided me with an HSI Investigative report authored by him, and an optical disc that contained files related to the investigation. The following is a summary of SA Westover's report:

A. The HSI-Milwaukee field office obtained lead information from HSI-Grand Forks, North Dakota, regarding an email account identified through computer forensics that was conducted as a result of search warrants executed in April 2014, and were related to child pornography investigations in North Dakota. Specifically, three separate email messages with attachments that contained video and or image files depicted children engaged in sexually explicit conduct were received by the email account mjx1990x@yahoo.com.

B. HSI-Grand Forks, North Dakota, determined a total of 18 attachment files, which contained child pornography, were sent in three different emails, from an email account utilizing the user name "cherrylollipops" to a distribution list of recipients, which included the email address mjx1990x@yahoo.com. The first email was sent on May 31, 2013, at 2:39 a.m., with two video files attached. The second email was sent on June 2, 2013, at 2:01 a.m., and contained

15 image file attachments. The third email was sent on July 25, 2013, at 2:41 p.m., with one video file attached.

C. Records obtained from Yahoo! Inc., pursuant to a summons on August 15, 2014, provided the following details regarding the email account mjx1990x@yahoo.com:

Created on November 16, 2012
Registered from IP address: 98.144.122.252
User name: MJ Walker
Alternate Communication Channels: mjx1988x@yahoo.com
Unverified

D. Login history showed the email account repeatedly accessed from IP address 98.144.122.252, between September 3, 2013, and January 8, 2014. The account was subsequently accessed numerous times from IP address 65.31.139.88, between January 21, 2014, and July 24, 2014. The most recent IP address 75.86.170.55 was used to access the account numerous times from August 1, 2014, through August 25, 2014.

E. Records from Time Warner Cable, pursuant to a DHS Summons on October 7, 2014, showed that IP addresses 65.31.139.88 and 75.86.170.55, were assigned to the same Internet account, which was activated on October 18, 2012, and was listed as still active as of the date of the response. The subscriber name for the Internet account identified as being associated with the two IP addresses on the corresponding dates and times was:

Sherry Craig
Subscriber address for the account as:
6412 103rd Ave. (Target Location)
Kenosha, WI, 53142
Associated telephone numbers:
262-891-3088
630-569-0583

F. Investigation related to telephone number 630-569-0583 revealed a connection to the Facebook profile of Sherry Caesar Craig (https://www.facebook.com/scraig8877). A review of the profile indicated Sherry was married to Bob Craig and they have two sons, Andrew and Brendon Craig. Further investigation revealed Sherry L. Craig (DOB XX/05/63), and Robert S. Craig (DOB XX/14/56), reside at the Target Location. Record checks indicated a birth date of XX/ 19/ 97, for Andrew Craig.

7. On November 10, 2015, I reviewed the optical disc related to this investigation that SA Westover had provided to me, which included three different emails that contained the 18 total files of children pornography.

A. I reviewed the two videos that were attached to the first identified email that mjx1990x@yahoo.com received on May 31, 2013 at 2:39 a.m., and observed the following:

The first attached video file labeled as "_," is approximately 42 seconds long, and it starts with a naked, prepubescent white female who is visible from approximately her lower chest down. She is lying on her back, on beige colored carpeting. Her legs are spread apart and her vagina is the focal point of the camera. She is small in stature, her genital area has no apparent pubic hair on, or around it, and her thighs appear to be undeveloped. An adult male, who appears to be naked, is kneeling between her legs, and appears to attempt to insert his erect penis into her anus. As the adult male is attempting to do this, he grabs her left thigh with his right hand. The hand of the adult male appears to be wider than tbe thickest part of the thigh of the child. At approximately 17 seconds into the video, the male appears to give up on the attempt to penetrate the child's anus and begins to attempt to insert his penis into her vagina. At approximately 27 seconds into the video, the male ejaculates on the child's pubic mound area and continues to rub his penis on the child's genitals, until the video ended.

The second attached video file labeled as "111816408918512_30868," is approximately 12 seconds long and it starts with a naked, prepubescent, white female lying on a bed with white sheets; she is on her back, with a pillow under her buttocks area, and her legs are up in the air and spread. An adult male, who appears to be nude outside of wearing what appears to be a pair of black dress socks, is kneeling between the girl's legs and holding them up. The male appears to be penetrating the child's genital area. The child is making facial expressions consistent with discomfort as this occurs.

B. I reviewed the 15 still images that were attached to the second identified email that mjx1990x@yahoo.com received on June 2, 2013, at 2:01 a.m., and observed the following:

Each of the child pornography images was of what appeared to be naked prepubescent and pubescent white females.

The image labeled "3576c6de1f98b78a0aba7c4ec792be11-1," depicts a naked prepubescent white female, sitting on the lap of a clothed pubescent female that is sitting on a chair in a bedroom which is decorated in a manner consistent with a juvenile female's bedroom. The prepubescent girl has no apparent pubic hair on or around her genital area, is overall small in stature and shows little, to no, breast development. The girl's legs are spread apart exposing her vagina and anus. The pubescent female has both of her hands placed near the pubic mound of the girl, and appears to be spreading apart the outer lips of the girl's vagina. The focal point of the image is the genital area of the girl.

The image labeled "th_844565384_1346844565_123_11lo-1," depicts a white prepubescent female, wearing a yellow T-shirt, and she is naked from the waist down. The girl is lying on a wood floor, with her legs spread apart, exposing her bare vagina and anus. She is touching her vagina with the fingers of her right hand. Part of the child's face is visible in the

image. She appears to be young, small in stature, and has no apparent pubic hair in, or around, her genital area. The focal point of the image is the genital area of the girl.

The image labeled "th_100203297_34645_123_513lo," depicts a naked, white, prepubescent female lying on her back in a bathtub. The child's legs are up and spread apart, exposing her bare vagina and anus. The face of the child is visible in the image, but appears to be purposely blurred out. The child is small in stature, has no apparent breast development, or pubic hair in, or around her genital area. The focal point of the image is the genital area of the child.

C. I reviewed the one video attached to the third identified email received on July 25, 2013, at 2:41 p.m., by mjx1990x@yahoo.com and observed the following:

The video is labeled "Dad girl," and it is approximately 2 minutes and eight seconds long. The video begins with a naked, prepubescent, white minor female on a bed with white sheets. She is small in stature, her genital area does not have apparent pubic hair on, or around it, and little to no breast development. The girl is bent over leaning on her elbows and on her knees. There is an adult white male who appears to be nude, with the exception of black dress type socks, kneeling on the bed behind the child and he appears to be penetrating her vagina with his erect penis. The male then appears to penetrate the anus of the child with his erect penis. The video continues with the male penetrating the anus of the child. While being penetrated, the child appears to be distracting herself by playing with objects on the bed, near her face. At approximately 1 minute and 35 seconds, the man stopped penetrating the child, got off of the bed, and walked out of the frame of the camera. The child then rolled over onto her back. At approximately 1 minute and 39 seconds, the scene changed, and it appears the same girl and

adult male are depicted. At this time, the child is on her back, and the man appears to penetrate the girl's anus with his erect penis. The video continued in this manner until the end.

8. On January 29, 2016, I received and reviewed National Center for Missing and Exploited Children (NCMEC) CyberTipline report number 7765259, which was sent to NCMEC by Facebook. The tip is summarized as follows:

An image of suspected child pornography was uploaded to a Facebook account and then sent to another Facebook user account on July 7, 2015 at 15:25:04 UTC. The Facebook account that uploaded and sent the image utilized IP address 75.86.162.222. The same Facebook account had a login IP address of 75.86.162.222 on December 24, 2015 at 06:14:38 UTC. NCMEC reported that the suspect IP address geo-located to the city of Kenosha, Wisconsin area, and belonged to Time Warner Cable/Internet LLC. Facebook provided the following user information related to the account that uploaded the image:

Name:	MJ Walker
Date of Birth:	XX-06-1991
Approximate Age:	24
Email Address:	mjx1994@yahoo.com (Verified)
ESP User ID:	100004256115687
Profile URL:	http://www.facebook.com/people/mj-walker/100004256115687
IP Address:	75.86.162.222 (Login) 12-24-2015 06:14:38 UTC

I reviewed the image associated to the NCMEC CyberTipline report. It is a front shot of a pubescent, naked girl standing in front of a shower curtain with her hands on her stomach below her navel, but above her bare vagina. The girl is the focal point of the image.

9. I utilized the American Registry for Internet Numbers (ARIN) to search IP address 75.86.162.222 and observed it was assigned to Time Warner Cable/Internet LLC. A search of www.maxmind.com also showed IP address 75.86.162.222 was assigned to Time Warner Cable and geo-locating to the Kenosha, Wisconsin area.

10. On February 10, 2016, I obtained a subpoena for Time Warner Cable/Internet LLC records relating to the personal identifying information for the subscriber account assigned IP address 75.86.162.222 on December 24, 2015 at 06:14:38 UTC. Further, the subpoena requested all records showing the subscriber IP address historical logs, including how long the subscriber was assigned IP address 75.86.162.222, dating back to July 7, 2015 at 15:25:04 UTC. The information provided by Time Warner revealed:

> Target Details 75.86.162.222, 12/24/2015 6:14:00 AM, GMT, 0
> Subscriber Name: SHERRY CRAIG
> Subscriber Address: 6412 103RD AVE, KENOSHA, WI 53142-7856 (Target Location)
> Service Type - RR HSD Activate Date: 3/10/2015 Deactivate Date: Still Active
> User Name or Features: sherrycraig@wi.rr.com
> Phone number: (262)891-3088, (630)569-0583
> Other Details
> Other Information: IP lease information: Original Lease start: 3/25/2015

11. After reviewing the subscriber information, I made telephone contact with E. Oliver, the Time Warner Internet/Cable Subpoena Analyst who had compiled the requested subscriber records. Oliver advised that the information provided in the "other details" section of the subpoena response, showed that the IP address 75.86.162.222, had been continually assigned to this subscriber account since March 25, 2015.

12. On February 17, 2016, at approximately 4:00 p.m., I and another SA conducted surveillance at the Target Location and observed a silver minivan bearing Wisconsin license plate 103-ULS parked in the driveway of the residence.

13. Registration information through the Wisconsin Department of Justice-TIME information system for Wisconsin license plate 103-ULS revealed the following:

> 2008 Chrysler Town and Country Touring Ed Van Truck Silver/Aluminum
> VIN: 2A8HR54P08R767757
> Owner(s):
>
> Craig, Sherry Lynn

DOB: XX/05/1963
DL: C6207926378505
6412 103rd Ave. (Target Location)
Kenosha, WI 53142-7856

AND

Craig, Robert S
DOB: XX/14/1956
DL: C6207775625402
6412 103rd Ave. (Target Location)
Kenosha, WI 53142-7856

14. WE Energies utilities records reveal the subscribers for the Target Location, since October 2012, are Sherry and Robert Craig, with an associated telephone number of 630-569-0583.

15. On Monday, April 25, 2016, at approximately 5:00 p.m. I and another DCI SA were on surveillance in the area of the Target Location. At this time, I observed that the garage door was closed, and no vehicles were parked in the driveway. We drove around the block in an effort to locate an area to park and conduct surveillance. Upon driving southbound on 103rd Avenue, north of the intersection with 64th Street, at approximately 5:03 p.m., I observed the previously documented silver Chrysler Town and Country minivan bearing Wisconsin license plate 103-ULS parked in the driveway of the Target Location, and I observed the garage door was closing.

16. At approximately 5:12 p.m., I observed a woman, later identified as Sherry Craig, exit the front door of the Target Location and walk northbound on 103rd Avenue, to a mailbox, located on the northwest side of the intersection of 103rd Avenue and 64th Street. Sherry then ran back to the Target Location and entered through the front door.

17. At approximately 5:25 p.m., I observed a white Toyota Corolla bearing Wisconsin license plate 102-ULS pull into and park in the driveway of the Target Location. A short

time later, the residence garage door began to open, and a white male, later identified as Robert Craig, exited the Corolla. Robert was observed carrying what appeared to be a black computer bag, and he entered the garage of the residence.

18. While the garage door was open, I observed a blue Chevrolet Camaro bearing Wisconsin license plate 104-ULS, and a blue Saturn Sport Utility Vehicle bearing Wisconsin license plate 177-XCC; both vehicles were parked in the garage of the Target Location. All surveillance activities were terminated a short time later.

19. A check of the Wisconsin Department of Justice TIME system showed the three vehicles are owned by Sherry Lynn Craig and Robert S. Craig.

CONCLUSION

21. Based on my training and experience, and the totality of circumstances of this case, I believe there is probable cause to search the Target Location for evidence of the crimes of Receipt, Distribution and Possession of Child Pornography, committed in violation of Title 18, United States Code, Sections 2252 (a)(1), (a)(2) and (a)(4)(B). Additionally, there is probable cause to believe that evidence of the commission of criminal violation(s) of said statues is located in the Target Location described further in Attachment A. Attachment B to this affidavit, which is incorporated herein by reference, is a list of items that would be the subject of search and seizure at this location.

ATTACHMENT A

DESCRIPTION OF LOCATION TO BE SEARCHED

The Target Location at 6412 103rd Avenue, City of Kenosha, Kenosha County, Wisconsin, is more particularly described as a single family residence composed of white siding, a black asphalt type roof, black shudders, and concrete stairs which lead up to the dark red, front entry door. The front of the residence faces north east. A black asphalt type driveway butts up to 103rd Avenue, on the north east side of the property and runs south west, leading to the garage, which is attached to the front side of the residence. Above the garage door, affixed to the header, are four black numbers which display "6412." The south west side of the house has an exposed basement with a sliding patio type door. A red shed with white trim is located on the property, and is south east of the residence.

ATTACHMENT B

PROPERTY TO BE SEIZED AND SEARCHED

1. All records relating to violations of Title 18, United States Code, Sections 2252(a)(1) and (a)(2) (receipt and distribution of child pornography); and Title 18, United States Code, Section 2252(a)(4)(B) (possession of child pornography), including:

a. Any and all notes, documents, records, or correspondence, in whatever form, pertaining to the above stated violations;

b. Any and all correspondence, in whatever form, identifying persons transmitting, receiving or possessing, through interstate commerce including by U.S. Mails or by computer, any visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2);

c. Any and all records, documents, invoices and materials that concern any accounts with YouTube, Google, KIK, Verizon or any other Internet Service Provider, screen names or email accounts;

d. Any and all visual depictions of minors, to include depictions of minors engaged in sexually explicit conduct, nude pictures, and modeling;

e. Any and all address books, mailing lists, supplier lists, mailing address labels, and any and all documents and records pertaining to the preparation, purchase, and acquisition of names or lists of names, in any way related to child pornography;

f. Any and all documents, records, or correspondence pertaining to occupancy or other connection to the Target Location;

g. Any and all diaries, notebooks, notes, pictures, emails, chats, directions, maps, banking, travel, documents, and any other records reflecting personal contact and any other activities with minors;

h. Any and all notes, documents, records, photos or correspondence that indicate a sexual interest in children, including, but not limited to:

i. Correspondence with children;

ii. Any and all visual depictions of minors;

iii. Internet browsing history;

iv. Books, logs, emails, chats, diaries and other documents.

2. Any and all web cameras, video cameras, videotapes, cameras, film, cell phones with cameras and/or Internet capability, or other photographic equipment that are instrumentalities of and/or contain evidence related to the above stated violations;

3. Computers or storage media used as a means to commit the violations described above;

4. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (bereinafter, "COMPUTER"):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. evidence of counter-forensic programs (and associated data) tbat are designed to eliminate data from the COMPUTER;

h. evidence of the times the COMPUTER was used;

i. passwords, encryption keys, and other access deviees that may be necessary to access the COMPUTER;

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records of or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

m. contextual information necessary to understand the evidence described in this attachment.

5. Routers, modems, and network equipment used to connect computers to the Internet.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, personal data assistants, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.